

JOSÉ A. CABRANES, *Circuit Judge*, joined by DENNIS JACOBS, REENA RAGGI, and CHRISTOPHER F. DRONEY, *Circuit Judges*, dissenting from the order denying rehearing *en banc*:

An evenly-divided *en banc* court has declined to rehear a case that presents multiple questions of exceptional importance to public safety and national security.<sup>1</sup> I respectfully dissent.

The panel majority quashed a warrant issued under section 2703 of the Stored Communications Act (“SCA”)<sup>2</sup> by a judicial officer of the United States upon a showing of probable cause. It erroneously concluded that the government’s use of an SCA warrant to require a United States-based service “provider” (Microsoft) to disclose the contents of a customer’s emails stored on servers located in Ireland was an extraterritorial application of the SCA.<sup>3</sup> The

---

<sup>1</sup> We have had occasion to observe that the decision to deny rehearing *en banc* “does not necessarily mean that a case either lacks significance or was correctly decided. Indeed, the contrary may be true. An oft-cited justification for voting *against* rehearing, perhaps counterintuitively, is that the case is ‘too important to *en banc*.’” *United States v. Taylor*, 752 F.3d 254, 256 (2d Cir. 2014) (quoting James L. Oakes, *Personal Reflections on Learned Hand and the Second Circuit*, 47 STAN. L. REV. 387, 392 (1995)) (emphasis in original). Accordingly, a reader should not give “any extra weight to a panel opinion in light of such a decision, inasmuch as the order denying rehearing may only reflect, for some judges, a general aversion to *en banc* rehearsings or faith in the Supreme Court to remedy any major legal errors.” *Id.* at 257.

<sup>2</sup> See 18 U.S.C. §§ 2701–12.

<sup>3</sup> See Majority Op. at 42.

panel majority ignored the fact that Microsoft lawfully had possession of the emails; that Microsoft had access to the emails in the United States; and that Microsoft's disclosure of the emails to the government would take place in the United States. In its unprecedented ruling, the panel majority has indisputably, and severely, restricted "an essential investigative tool used thousands of times a year [in] important criminal investigations around the country."<sup>4</sup> To top this off, the panel majority's decision does not serve any serious, legitimate, or substantial privacy interest.<sup>5</sup>

## I.

The negative consequences of the panel majority's opinion are far reaching. It has substantially burdened the government's legitimate law enforcement efforts; created a roadmap for the facilitation of criminal activity;

---

<sup>4</sup> Petition for Rehearing and Rehearing En Banc ("En Banc Petition") 2–3. In just the second half of 2015, Google alone "received 3,716 warrants seeking data from a total of 9,412 accounts." *Id.* at 18.

<sup>5</sup> In his concurring opinion, Judge Lynch observes that despite Microsoft's suggestion that "this case involves a government threat to individual privacy . . . uphold[ing] the warrant here would not undermine basic values of privacy as defined in the Fourth Amendment and in the libertarian traditions of this country." Concurring Op. at 1. As he explains, "the government complied with the most restrictive privacy-protecting requirements of the [SCA]. Those requirements are consistent with the highest levels of protection ordinarily required by the Fourth Amendment for the issuance of search warrants." *Id.* at 2.

and impeded programs to protect the national security of the United States and its allies.<sup>6</sup>

First, as Judge Lynch's concurring opinion explains, the panel majority's holding affords "absolute" protection from disclosure to electronic communications stored abroad, regardless of whether they are controlled by a domestic service provider and are accessible from within the United States.<sup>7</sup> As a result, the government can "never obtain a warrant" that would require a service provider to turn over emails stored in servers located outside the United States, regardless of how "certain [the government] may be that [emails] contain

---

<sup>6</sup> Judge Carney's opinion concurring in the order denying rehearing *en banc* does not dispute the fact that the panel majority's decision has put the safety and security of Americans at risk. Instead, in a footnote, the concurring opinion notes two sections of the SCA that it believes lessen the severity of these consequences. *Ante* at 1 n.2 (Carney, J., concurring in the order denying reh'g *en banc*). The first section, 2702(b)(8), permits "[a] provider . . . [to] divulge the contents of a communication . . . to a government entity, *if the provider*, in good faith, believes that" there are exigent circumstances. *Id.* (quoting 18 U.S.C. § 2702(b)(8)) (emphasis added). The second section, 2703(e), "gives a provider immunity from civil liability for a voluntary production of content made 'in accordance with . . . [a] statutory authorization . . .'" *Id.* at 2 n.2 (quoting 18 U.S.C. § 2703(e)). In asking us to entrust our national security to the good faith of internet service providers, I can only assume that the concurring opinion has some unstated reason for believing that Microsoft is just an atypically unpatriotic service provider and that other, more virtuous, service providers would never put their business interests ahead of public safety and national security.

<sup>7</sup> Concurring Op. at 4.

evidence of criminal activity, and even if that criminal activity is a terrorist plot.”<sup>8</sup>

Second, the panel majority’s opinion has created a roadmap for even an unsophisticated person to use email to facilitate criminal activity while avoiding detection by law enforcement. The Microsoft customer targeted by the government’s warrant in this case indicated to Microsoft when he signed up for its service that he resided in Ireland—a representation Microsoft took at face value.<sup>9</sup> Because Microsoft has a policy of “stor[ing] a customer’s email information . . . at datacenters located near the physical location identified by the user as its own,” Microsoft automatically stored his emails on its servers in Ireland—now safely beyond the reach of an SCA warrant.<sup>10</sup> Based on the panel majority’s holding, a criminal who resides in the United States can now check the proverbial “box” informing Microsoft that he resides in another country when signing up for service—perhaps a country without a Mutual Legal Assistance

---

<sup>8</sup> *Id.* at 4–5.

<sup>9</sup> Majority Op. at 8–9.

<sup>10</sup> *Id.*

Treaty (“MLAT”) with the United States<sup>11</sup>—and thereby avoid having his emails disclosed to the government pursuant to an SCA warrant.

Third, the panel majority’s decision has already led major service providers to reduce significantly their cooperation with law enforcement. The panel majority held that the physical location of a server containing a customer’s emails determines whether an SCA warrant seeking the disclosure of those emails is an extraterritorial application of the SCA. However, electronic data storage is more complex and haphazard than the panel majority’s holding assumes. Many service providers regularly “store different pieces of information for a single customer account in various datacenters at the same time, and routinely move data around based on their own internal business practices.”<sup>12</sup> Still other providers are unable to determine “where particular data is stored or whether it is stored outside the United States.”<sup>13</sup> Consequently, in an effort to

---

<sup>11</sup> The United States has entered into MLATs with several countries, allowing parties to the treaty to request assistance with ongoing criminal investigations, including issuance and execution of search warrants. *See id.* at 41. However, many countries do not have MLATs with the United States, *e.g.*, Indonesia and Pakistan, and law enforcement cooperation with those countries is limited. *See* Gov’t Br. 48–53 (describing the inefficiencies of the MLAT process as well as its ineffectiveness in certain circumstances).

<sup>12</sup> En Banc Petition 18–19.

<sup>13</sup> *Id.*

apply the panel majority's confected holding to the technological realities of electronic data storage, major service providers are adopting restrictive disclosure policies that radically undermine the effectiveness of an SCA warrant.<sup>14</sup>

For example, Google will now disclose "only those portions of customer accounts stored in the United States at the moment the warrant is served."<sup>15</sup> Google's policy is particularly troubling because "the only [Google] employees who can access the entirety of a customer's account, including those portions momentarily stored overseas, are located in the United States."<sup>16</sup> As a result, law enforcement might never be able obtain data stored in Google servers abroad, even with the help of an MLAT.

Yahoo! has advised law enforcement that it "will not even preserve data located outside the United States in response to a [s]ection 2703 request."<sup>17</sup> This policy, as the government points out in its En Banc Petition, creates "a risk that

---

<sup>14</sup> See *Id.* 17–19; see also Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, WASH. POST: THE VOLOKH CONSPIRACY (Nov. 29, 2016), <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case>.

<sup>15</sup> En Banc Petition 19.

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

data will be moved or deleted before the United States can seek assistance from a foreign jurisdiction, much less actually serve a warrant and secure the data.”<sup>18</sup>

## II.

The baleful consequences of the panel’s decision are compelled neither by the text of the statute nor by our precedent. The panel majority arrived at its damaging holding because it adopted a flawed reading of the SCA.

The second step of the two-step framework for analyzing extraterritoriality issues set forth in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010), and *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016), was the determinative issue in this case.<sup>19</sup> At step two, a court must “determine whether

---

<sup>18</sup> *Id.*

<sup>19</sup> The first step of the extraterritorial analysis is “to determine whether the relevant statutory provision contemplates extraterritorial application.” Majority Op. at 22 (citing *Morrison*, 561 U.S. at 262–65). Because the government conceded at oral argument that the SCA lacks extraterritorial application, *id.*, there is no need to pursue the point. To the extent the panel majority did so in a lengthy discussion of the SCA’s use of the word “warrant” in section 2703, *see id.* at 25–31, which then informs its step-two “focus” analysis, it is appropriate to note concern with the reasoning.

The panel majority conflates SCA disclosure warrants with traditional search warrants. While the latter authorize government action as to *places*, the former authorize government action on *persons*. The fact that warrants generally do not authorize government searches of places outside the United States—a limitation grounded in respect for sovereignty, not privacy, *see, e.g., The Apollon*, 22 U.S. (9 Wheat.) 362, 371 (1824) (Story, J.); Restatement (Third) of Foreign Relations Law § 432(2); *see also In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 167–72 (2d Cir. 2008)—does not support a conclusion that warrants are impermissibly applied extraterritorially

the case involves a domestic application of the statute,” which “we do . . . by looking to the statute’s ‘focus’” and by identifying where “the conduct relevant to the statute’s focus occurred.”<sup>20</sup> Here, the panel majority explained that the “focus” of the SCA is user privacy,<sup>21</sup> and in a single sentence, identified the location of the conduct relevant to that focus: “[I]t is our view that the invasion of the customer’s privacy takes place under the SCA where the customer’s protected content is accessed—here, where it is seized by Microsoft, acting as an

---

when they compel persons within the United States to disclose property lawfully in their possession anywhere in the world. *Cf. Linde v. Arab Bank, PLC*, 706 F.3d 92, 109 (2d Cir. 2013) (Carney, J.) (observing that the Supreme Court has held that “the operation of foreign law ‘do[es] not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that [law].” (quoting *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court*, 482 U.S. 522, 544 n. 29 (1987)). In that sense, a disclosure warrant is more akin to a subpoena, *see, e.g., Marc Rich & Co. A.G. v. United States*, 707 F.2d 663, 668–70 (2d Cir. 1983) (holding that persons in the United States can be required to retrieve subpoenaed material from abroad), *but* with the important added protection of a probable cause showing to a neutral magistrate. Thus, the panel majority is simply wrong in concluding that “a warrant protects *privacy* in a distinctly territorial way.” Majority Op. at 26 (emphasis added). Warrants protect privacy through the Fourth Amendment requirement that they issue only upon probable cause. *See* Concurring Op. at 1–3.

By failing to distinguish between search warrants as to places and disclosure warrants directed to persons, and between sovereignty and privacy, the panel majority construes “warrant” as used in the SCA to yield the perverse result of affording greater privacy protection to foreign nationals and Americans who say they reside abroad than to resident United States citizens with respect to electronic communications in the lawful possession of a United States service provider.

<sup>20</sup> *RJR Nabisco*, 136 S. Ct. at 2101.

<sup>21</sup> *See* Majority Op. at 32–39.



agent of the government.”<sup>22</sup> Because the emails at issue were stored on a server in Ireland, the panel majority concluded that the warrant seeking the disclosure of those emails was an extraterritorial application of the SCA.<sup>23</sup> Not so.

Even if the “focus” of the SCA is user privacy, a plain reading of the statute makes clear that the conduct relevant to the SCA’s “focus,” and which the SCA seeks to regulate, is a provider’s *disclosure* or *non-disclosure* of emails to third parties, not a provider’s *access* to a customer’s data. Here, Microsoft’s disclosure

---

<sup>22</sup> *Id.* at 39. Judge Carney’s opinion concurring in the order denying rehearing *en banc* reiterates the panel majority’s conclusion—that, “the locus of the SCA’s privacy protections [is] at the place of data storage”—but again provides little or no explanation for how or why the statutory language permits such a reading. *Ante* at 4 (Carney, J., concurring in the order denying reh’g *en banc*). It offers only the sphinx-like explanation that “§ 2701, by proscribing unauthorized access to storage facilities, not only limits disclosure but also ‘shelters the communications’ integrity.” *Id.* at 5 (quoting Majority Op. at 35). Conversely, and as the concurring opinion itself notes, those of us dissenting from the denial of *en banc* review “offer[ ] a detailed recitation of the available statutory support for [the] conclusion” that the conduct relevant to the SCA’s focus occurs at the place of disclosure. *Id.* at 6.

<sup>23</sup> Judge Carney’s *en banc* concurrence asserts that the panel majority’s “reading of the SCA did no more than adhere to the dictates of *Morrison* in construing the SCA.” *Ante* at 3 (Carney, J., concurring in the order denying reh’g *en banc*). I disagree. Instead of locating support for its legal conclusion in the text or structure of the SCA, the concurring opinion, like the panel majority’s opinion, fixates on its unsubstantiated belief that the warrant at issue here raises “concerns of sovereignty and international comity.” *Id.* at 4. They both then conclude, based primarily on that misconception, that the warrant at issue must be an extraterritorial application of the SCA. *Morrison*, however, does not permit a court to conclude that a particular application of a statute is extraterritorial simply because it believes that the application threatens international comity. Rather, step two of the *Morrison* framework directs courts to examine the statutory language. *See Morrison*, 561 U.S. at 266–67.

of emails to the government would take place at its headquarters in the United States. Therefore, had the panel majority correctly identified the conduct relevant to the SCA's "privacy focus," it would have concluded that the warrant at issue was a domestic application of the SCA.<sup>24</sup>

A brief examination of the text and structure of the SCA leads inexorably to the conclusion that the conduct relevant to the SCA's "privacy focus" is its regulation of *disclosures* by providers to third-parties. As the panel majority

---

<sup>24</sup> According to the *en banc* concurrence, the panel majority considered and rejected my suggested holding partly because that holding "ignores situations in which the effects outside the United States are less readily dismissed." *Ante* at 8 (Carney, J., concurring in the order denying reh'g *en banc*). As far as I understand it, the concurring opinion asserts the belief that the facts of this case are too sympathetic to my interpretation of the law and that only under alternative, entirely fictional, circumstances would the true menace of my position be revealed. It then devises a hypothetical warrant that purports to show how my suggested holding permits the authorization of warrants with too limited a nexus to the United States: an SCA warrant requiring a "United States . . . branch office of an Irish service provider" to disclose electronic information stored in Ireland but accessible in the United States that belonged to an account "opened and established in Ireland by an Irish citizen," the disclosure of which would breach Irish law. *Id.*

This hypothetical is too clever by half. In attempting to construct the most shocking warrant conceivable, the concurring opinion omits two critical facts, both of which are required under my understanding of the law. First, a judicial officer of the United States would have to issue the warrant upon a finding of probable cause to believe that the information being sought was related to criminal activity occurring within the United States. Second, the provider would have to disclose the targeted information to the government inside the United States. Thus, if all of the conditions necessary for a valid SCA warrant are satisfied, there is no basis for concluding that even Judge Carney's imagined warrant, not to mention the warrant at issue, is an extraterritorial application of the SCA.

observes, “the first three sections of the SCA contain its major provisions.”<sup>25</sup> The first of those sections, section 2701, addresses “[u]nlawful access to stored communications.”<sup>26</sup> Section 2701 is the *only* major provision of the SCA to specifically limit *access* to customer communications. Although the panel majority fails to explain adequately why the “invasion of the customer’s privacy takes place . . . where the customer’s protected content is *accessed*,”<sup>27</sup> section 2701 is the only plausible textual basis for the panel majority’s bizarre holding.

However, while section 2701 prohibits “[u]nlawful access” (most obviously hacking), it recognizes that providers have standing authority to *access* a customer’s electronic communications.<sup>28</sup> In fact, section 2701(c) expressly exempts from its restrictions on *access* “conduct authorized . . . by the person or entity providing a wire or electronic communications service,” *i.e.*, the provider.<sup>29</sup> It is unreasonable, therefore, for the panel majority to conclude that a provider’s

---

<sup>25</sup> *Id.* at 35; *see* 18 U.S.C. §§ 2701–03

<sup>26</sup> 18 U.S.C. § 2701.

<sup>27</sup> Majority Op. at 39 (emphasis added).

<sup>28</sup> 18 U.S.C. § 2701

<sup>29</sup> *Id.* § 2701(c)(1) (emphasis added).

lawful access to a customer's emails is the conduct relevant to the SCA's "privacy focus."<sup>30</sup>

On the other hand, section 2702 expressly prohibits, with some exceptions, a provider from "*disclos[ing]*" a customer's communications.<sup>31</sup> For example, section 2702(a) sets forth three "[p]rohibitions" that must be followed by service providers like Microsoft.<sup>32</sup> Each prohibition states that the provider "shall not knowingly *divulge*" certain information, such as the contents of a communication, unless an exception in subsection (b) or (c) applies.<sup>33</sup> In turn, section 2703 specifically empowers the government to "require the *disclosure* by a provider . . . of the contents of a[n] . . . electronic communication . . . pursuant to a warrant."<sup>34</sup>

Considering sections 2701, 2702, and 2703 together, it is clear that the SCA protects user privacy by prohibiting unlawful access of customer communications (such as hacking), and by regulating a provider's *disclosure* of

---

<sup>30</sup> The panel majority characterizes a service provider that "access[es]" a user's email pursuant to an SCA warrant as "an agent of the government." Majority Op. at 29, 39. But, the legal authorities cited by the panel for the proposition that a private party who assists the government in conducting a search and seizure "becomes an agent of the government," *id.* at 29, do not involve circumstances, such as those here, where the private party already had possession of the relevant property.

<sup>31</sup> *Id.* §§ 2702–03 (emphasis added).

<sup>32</sup> *See id.* § 2702(a)(1)–(3).

<sup>33</sup> *Id.* (emphasis added).

<sup>34</sup> *Id.* § 2703(a) (emphasis added).

customer communications to third parties. Inasmuch as section 2701's limitations on *access* specifically do not apply to providers, it is only when a provider *divulges* the content of a user's communication to a third party that the provider puts a user's privacy at risk. It is not a mere coincidence that the SCA recognizes a provider's standing authority to *access* a user's communications and, at the same time, prohibits a provider from *disclosing* those communications to third-parties except as authorized by sections 2702 and 2703. Accordingly, the panel majority's focus on *access* (instead of on *disclosure*) is entirely misplaced.<sup>35</sup>

Put another way, Microsoft did not need a warrant to take possession of the emails stored in Ireland. Nor did it need a warrant to move the emails from Ireland to the United States. It already had possession of, and lawful *access* to, the targeted emails from its office in Redmond, Washington. Only Microsoft's

---

<sup>35</sup> Neither the panel majority's opinion nor the *en banc* concurrence explains why "privacy" is better served by looking to a provider's *access* rather than its *disclosure*. They just assume the point. *See ante* at 13 (Carney, J., concurring in the order denying reh'g *en banc*) ("The better approach . . . is one that looks to the step taken before disclosure—access—in determining privacy's territorial locus."); Majority Op. at 39. Both the panel majority's opinion and the *en banc* concurrence also fail to explain why the physical location of the datacenter is the legal point of *access*, rather than the location from where the service provider electronically gains *access* to the targeted data, which, in this case, is the United States. Evidently, it is so (again) because the panel majority and the concurrence say it is so. *See ante* at 4 (Carney, J., concurring in the order denying reh'g *en banc*) ("[T]he locus of the SCA's privacy protections [is] at the place of data storage."); Majority Op. at 39. Naked assertions, however, do not the law make.

*disclosure* of the emails to the government would have been unlawful under the SCA absent a warrant.<sup>36</sup>

\*\*\*

In sum, the government obtained a warrant based on a showing of probable cause before a judicial officer of the United States. That warrant required Microsoft's office in Redmond, Washington, to disclose certain emails that happened to be electronically stored in its servers abroad, but to which Microsoft had immediate access in the United States. Because the location of a provider's *disclosure* determines whether the SCA is applied domestically or extraterritorially, the enforcement of the warrant here involved a domestic application of the SCA. The panel should have affirmed the District Court's denial of Microsoft's motion to quash.

For the foregoing reasons, I dissent from the order denying rehearing *en banc*. I trust that the panel's misreading of this important statute can be rectified

---

<sup>36</sup> To the extent the panel majority concludes that the SCA does not apply extraterritorially to compel a provider's disclosures pursuant to section 2703, its place-of-access reasoning raises concerns about the extraterritorial reach of protections from unlawful access and disclosures afforded by sections 2701 and 2702. Such a concern might be avoided if the statute is construed to reach, at least, the conduct of persons within the jurisdiction of the United States. This further concern only reinforces the need for *en banc* review.

as soon as possible by a higher judicial authority or by the Congress of the United States.<sup>37</sup>

---

<sup>37</sup> Ultimately, Judge Carney's concurring opinion suggests that rehearing *en banc* is unnecessary because the panel majority's holding was compelled by an anachronistic statute and an inflexible framework for analyzing questions of extraterritoriality. *Ante* at 13–14 (Carney, *J.*, concurring in the order denying reh'g *en banc*). It also notes that some Members of Congress have introduced a bill purporting to resolve all of our concerns with the statute. *Id.* at 2 n.3. I submit that rehearing *en banc* is necessary precisely because the panel majority misread the SCA and misapplied the extraterritoriality framework set forth in *Morrison*. Where a decision of our court has unnecessarily created serious, on-going problems for those charged with enforcing the law and ensuring our national security, and where a legislative remedy is entirely speculative, we should not shirk our duty to interpret an extant statute in accordance with its terms.